UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/818,802	03/27/2001	Tetsuya Noguchi	JP920000026US1	9893

48233 7590 01/03/2011

SCULLY, SCOTT, MURPHY & PRESSER, P.C.
400 GARDEN CITY PLAZA
SUITE 300
GARDEN CITY, NY 11530

EXAMINER	
LEE, JASON T	

ART UNIT	PAPER NUMBER
2438	

NOTIFICATION DATE	DELIVERY MODE
01/03/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

IBMPAIRENotify@ssmp.com

Office Action Summary	Application No.	Applicant(s)	
	09/818,802	NOGUCHI ET AL.	
	Examiner	Art Unit	
	JASON LEE	2438	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 October 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5-12 and 14-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5-12 and 14-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application.
6) ☐ Other: _____.

DETAILED ACTION

1. The following is a final action in response to applicant's amendments filed on October 25, 2010. Claims 1, 10, 16, 18 and 20 have been amended. Claims 4 and 13 has been cancelled previously. No claim has been added. At this time, claims 1-3, 5-12 and 14-24 are pending and addressed below.

Response to Arguments

2. Applicant's amendments are sufficient to overcome the claim objections for claims 20-24. Applicant has amended the claims as suggested in the previous office action, therefore the claim objection for claims 20-24 has been withdrawn. However, claim 17 recites " The proving system **according to-claim 16**, wherein said means for accepting said certificate includes means for providing an electronic signature for said certificate." where **to-claim** believed is a typographic error. Claim 19 recites " The system according to claim 18, wherein said means **9** for generating said certificate includes means for providing an electronic signature for said certificate." Where **9** is also believed a typographic error. Appropriates action is needed.

3. Applicant's amendments are sufficient to overcome the 35 U.S.C. 112 second paragraph, rejections for claims 1,10,16,18 and 20 set forth in the previous office action. Applicant amended the claim language to remove the "said" word and remove the insufficient antecedent basis. Therefore, the 112 rejections for claims 1, 10, 16, 18 and 20 have been withdrawn.

4. Applicant's arguments relating to Vaeth, Kobata and DeBry fail to disclose the newly amended claim 1 has been fully considered but are moot in view of the new ground(s)

of rejection necessitated by amendment. Newly amended claim 1 now incorporates added limitations of "**synchronizing clocks of said proof service provider with said witness**". Therefore, the scope of the claims has changed. Accordingly, new art is being used to address the newly added limitation. Van der Kaay et al (US 6,393,126 B1) has been introduced to address the newly amended limitations. Please see the new grounds of the rejections in this office action.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-3, 5-12, 14-15, 18-22 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vaeth et al (6,308,277); in view of Kobata et al. (6,591,367); in view of DeBry (6,385,728) and further in view of Van der Kaay et al (US 6,393,126 B1).

As for claim 1:

Vaeth discloses **an electronic content proving method using a computer system or a computer network** (see Vaeth col. 1, lines 10-13 "the field of secure telecommunications, and, more specifically, the issuance and management of "certificates" in such telecommunications, particularly in electronic commerce.") **comprising the steps of: (a) a proof service provider transmitting a certificate generation request to a witness or a certificate generator;** (see Vaeth col. 6, lines 19-21 "the RA (a) accessing the certificate request information via the network")

(b) said witness or said certificate generator obtaining electronic content upon the receipt of said certificate generation request from said service provider; and

(c) generating a certificate, wherein said certificate includes address information for said electronic content and time information for a proof;

verifying a user's identity by referring to determine said user as an authenticated user; (see Vaeth col. 4, lines 18-26 “Where the registration database has been created and historically maintained and used independently of the use of a CA, for example, a credit card issuer's databases of credit card holders and merchants, the maintainer of the database likely has more experience with for verification of the identity of the party.” And col. 2, lines 40-45 “By applying this type of encryption to a shortened, unique representation of a communication generated by a "hash function", a "digital signature" can be generated that authenticates to holders of the public key that the sender/encoder of the communication is the holder of the associated private key.”)

verifying that a certificate has been prepared by said witness; (see Vaeth col. 4, lines 16-17 “the CA performs the identity verification function, albeit using the registration

database.”) **requesting preparation of a certificate by said witness;** (see Vaeth col. 4, lines 4- 5“CAs could have a "registration authority" (RA) function, for example, registering who within an organization was authorized with signing privileges relative to a certain level of transaction activity.” And col 4 line 34-36 "Requester 70 employs a public/private key pair generator 71 to generate the key pair, then prepares a certificate request data (CRD) submission 73, signed with the requester's private key, and sends it

to the LRA 80 using secure means 75.") **determining whether said witness has accepted said witness;** (see Vaeth col. 6, lines 18-20 "the RA (a) accessing the certificate request information via the network, (b) approving the request, and (c) sending the approval to the CA via the network;") **synchronizing clocks of said proof service provider with said witness; and accepting said certificate from said witness.** (see Vaeth col. 4, lines 40-42 " LRA 80 then accepts CRD 73, checks it for errors or omissions and verifies the requester's signature, submitting it to CA 90 in a message signed by LRA 80 using secure means 81.") Vaeth discloses administering certificates digitally signed by a trusted entity (certificate authority) to ensure that certificated transactions are authenticated as that of a particular entity. Requests for a certificate, along with verification information, are directed to the certificate authority, where they are held and accessed by an entity having verification responsibilities (registration authority). (see Vaeth abstract). Vaeth teaches the CA and RA are proof service provider and witness as the claim limitation recites.

Vaeth does not disclose the step of the witness or certificate generator obtaining electronic content upon the receipt of the certificate generation request from the service provider. However, Kobata discloses **for transmitting digital information over a network** (Kobata: col. 1, lines 1-2 "transmitting digital information over a network") **comprising receiving system obtains digital information from a server system** (Kobata: Fig. 1; col. 3, lines 21-43; col. 4, lines 6-49).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of obtaining contents electronically as Kobata teaches in the system of Vaeth so as to save transmission bandwidth.

The combination of Vaeth and Kobata is silent on the teaching of including address information for said electronic content and time information for said proof in the certificate. DeBry is relied on for the teaching of **including address information for said electronic content and time information for said proof in the certificate** (DeBry: Fig. 2 and col 7 lines 20-31 "The will-call certificate 40 (FIG. 2) contains the following fields: distinguished name of the document source 41, which tells the print server exactly where to go to get the document (e.g., including the Internet address); the path to the document file 42 to find the document within the file system; and the digital signature of the provider of the document 43. When the document source created the will-call certificate, the document source digitally signed the will-call certificate using its own private key. The will-call certificate also contains a date indicating a date until which the certificate is valid 44, and a serial number for tracking purposes 45. ")

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of including address information for said electronic content and time information for said proof in the certificate in the system of Vaeth and Kobata, as DeBry teaches so as to securely retrieve a file.

The combination of Vaeth, Kobata and DeBry does not disclose "**synchronizing clocks of said proof service provider with said witness";** however, Van der Kaay discloses

this limitation. (see Van der Kaay col 2 lines 40-42 " a Time Calibration Certificate (TCCert), as used herein, which relates to the certification of a clock as synchronized with an accepted standard." And col 8 line 65 to col 9 line 24 "The NOC 210 comprises three additional functional components that implement the PKI authentication capability of the TTI system. The Registration Authority (RA) 312 associates each device in the TTI system with a name. In this manner, TTI devices can be identified, monitored, and controlled. The Certification Authority (CA) 314 associates a public key with each device using the name of the device provided by the RA 312....the NOC 210 acts as an RA 312 to the CA 314 for the issuance of digital certificates to the TTI elements. Each element within the TTI preferably has a distinguished name so that it may be uniquely identified.")

Van der Kaay discloses a Trusted Time Infrastructure (TTI) system provides time stamps, in the form of trusted temporal tokens, for electronic documents from a local source.A preferred embodiment of the system comprises a trusted master clock, a trusted local clock, and a network operations center. The trusted master clock and the network operations center are located within secure environments controlled by a trusted third party. The trusted local clock, which issues time stamps, is certified to be synchronized with the trusted master clock. (see Van der Kaay col 4 lines 40-51)

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the synchronizing clocks of said proof service provider with said witness (e.g. CA and RA) as taught by Van der Kaay to modify the modified-invention of

Vaeth because there are in the same field of endeavor of authentication for certification so as to securely verifying, processing, and storing the electronic content.

As for claim 2:

The combination of Vaeth, Kobata, DeBry and Van der Kaay discloses **the electronic content proving method according to claim 1, wherein said certificate includes said electronic content, or data that uniquely represent said electronic content.** (see Vaeth: Fig.1, col. 3, lines 35-41 "the CA provides a certificate including (a) information identifying the certified party, (b) the certified party's public key, and (c) information identifying the CA, digitally signed, that is, encrypted with the CA's private key. The certified party can send such a certificate.").

As for claim 3:

The combination of Vaeth, Kobata, DeBry and Van der Kaay discloses **the electronic content proving method according to claim 1, further comprising the step of (d) accumulating said certificate in said service provider or transmitting said certificate to a user.** (see Vaeth col 8 lines 49-51 "storing the certificate at 191, and notifying requester 170 of the availability of the certificate, for example, by e-mail over network 200.")

As for claim 5:

The combination of Vaeth, Kobata, DeBry and Van der Kaay discloses **the electronic content proving method according to claim 1, wherein said step of generating said certificate includes a step of providing a signature for said certificate; and wherein said step of providing a signature includes a first configuration process**

consisting of a first signature step by said witness or said certificate generator and a second signature step by said service provider, or a second configuration process consisting of a signature step by a notary service provider. (see Vaeth col. 4, lines 41-47 “LRA 80 then accepts CRD 73, checks it for errors or omissions and verifies the requester's signature, submitting it to CA 90 in a message signed by LRA 80 using secure means 81. CA 90 validates the request for a certificate, then prepares the certificate information, signs it with the CA's private key and distributes the certificate to subscribers 95”)

As for claim 6:

The combination of Vaeth, Kobata, DeBry and Van der Kaay discloses **the electronic content proving method according to claim 5, wherein said signature is encrypted using a public key encryption method to prevent alteration by a person other than a signer.** (see Vaeth col. 2, line 16 to col 3 line 13” General asymmetric or "public key" encryption/decryption mechanisms are well known in the art, such as those invented by Rivest, Shamir and Adleman ("RSA"). The concept is based upon the existence of algorithms that allow encryption/decryption using related "keys" that are associated with each other, but one of which, the "private" key, is extremely difficult to derive from the other, "public" key."; and col 3 lines 35-40 “the CA provides a certificate including (a) information identifying the certified party, (b) the certified party's public key, and (c) information identifying the CA, digitally signed, that is, encrypted with the CA's private key. The certified party can send such a certificate.”).

As for claim 7:

The combination of Vaeth, Kobata, DeBry and Van der Kaay discloses **the electronic content proving method according to claim 2, wherein said data that uniquely represents said electronic content is a hash code.** (see Vaeth col. 2, lines 40-45 "By applying this type of encryption to a shortened, unique representation of a communication generated by a "hash function", a "digital signature" can be generated that authenticates to holders of the public key that the sender/encoder of the communication is the holder of the associated private key." and col 2 hash function 45, 15)

As for claim 8:

The combination of Vaeth, Kobata, DeBry and Van der Kaay discloses **the electronic content proving method according to claim 1, wherein in accordance with a request from said user, said certificate generation request is transmitted to said witness or to said certificate generator on one or multiple dates, or is transmitted continuously during one or multiple specific periods.** (see Vaeth col. 6, lines 1-6 "(1) the requesters send their requests and verification data to the CA, (2) the RA accesses the requests and verification data held at the CA and performs the identity verification function at the RA, and (3) upon approval of the RA, the CA performs the certificate issuance function. ")

As for claim 9:

The combination of Vaeth, Kobata, DeBry and Van der Kaay discloses **the electronic content proving method according to claim 1, wherein synchronization of time is effected between said service provider and said witness or said certificate**

generator. (see Vaeth Fig. 2 elements 80 and 90, col. 4, lines 41-47 “LRA 80 then accepts CRD 73, checks it for errors or omissions and verifies the requester's signature, submitting it to CA 90 in a message signed by LRA 80 using secure means 81. CA 90 validates the request for a certificate, then prepares the certificate information, signs it with the CA's private key and distributes the certificate to subscribers 95”)

As for claim 10:

Vaeth discloses **a proving system for a service provider that proves oneness for perusal and non-alteration of an electronic content using a computer system or a computer network** (see Vaeth col. 1, lines 10-13 " the field of secure telecommunications, and, more specifically, the issuance and management of "certificates" in such telecommunications, particularly in electronic commerce.”)

comprising: means for transmitting a certificate generation request to a witness or a certificate generator; (see Vaeth col. 6, lines 19-21 “the RA (a) accessing the certificate request information via the network”)

means for obtaining electronic content upon the receipt of said certificate generation request from said service provider; and means for generating a certificate, wherein said certificate includes address information for said electronic content and time information for a proof;

means for verifying a user's identity by referring to a usage history to determine said user as an authenticated user; (see Vaeth col. 4, lines 18-26 “Where the registration database has been created and historically maintained and used independently of the use of a CA, for example, a credit card issuer's databases of credit

card holders and merchants, the maintainer of the database likely has more experience with for verification of the identity of the party." And col. 2, lines 40-45 "By applying this type of encryption to a shortened, unique representation of a communication generated by a "hash function", a "digital signature" can be generated that authenticates to holders of the public key that the sender/encoder of the communication is the holder of the associated private key.")

means for verifying that a certificate has been prepared by said witness; (see Vaeth col. 4, lines 16-17 "the CA performs the identity verification function, albeit using the registration database.") **means for requesting preparation of a certificate by said witness;** (see Vaeth col. 4, lines 4- 5"CAs could have a "registration authority" (RA) function, for example, registering who within an organization was authorized with signing privileges relative to a certain level of transaction activity." And col 4 line 34-36 "Requester 70 employs a public/private key pair generator 71 to generate the key pair, then prepares a certificate request data (CRD) submission 73, signed with the requester's private key, and sends it to the LRA 80 using secure means 75.") **means for determining whether said witness has accepted said witness process;** (see Vaeth col. 6, lines 18-20 "the RA (a) accessing the certificate request information via the network, (b) approving the request, and (c) sending the approval to the CA via the network;") **means for synchronizing clocks of said proof service provider with said witness; and accepting said certificate from said witness.** (see Vaeth col. 4, lines 40-42 " LRA 80 then accepts CRD 73, checks it for errors or omissions and verifies the requester's signature, submitting it to CA 90 in a message signed by LRA 80

using secure means 81.") Vaeth discloses administering certificates digitally signed by a trusted entity (certificate authority) to ensure that certificated transactions are authenticated as that of a particular entity. Requests for a certificate, along with verification information, are directed to the certificate authority, where they are held and accessed by an entity having verification responsibilities (registration authority). (see Vaeth abstract). Vaeth teaches the CA and RA are proof service provider and witness as the claim limitation recites.

Vaeth does not disclose the step of the witness or certificate generator obtaining electronic content upon the receipt of the certificate generation request from the service provider. However, Kobata discloses **for transmitting digital information over a network** (Kobata: col. 1, lines 1-2 "transmitting digital information over a network") **comprising receiving system obtains digital information from a server system** (Kobata: Fig. 1; col. 3, lines 21-43; col. 4, lines 6-49).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of obtaining contents electronically as Kobata teaches in the system of Vaeth so as to save transmission bandwidth.

The combination of Vaeth and Kobata is silent on the teaching of including address information for said electronic content and time information for said proof in the certificate. DeBry is relied on for the teaching of **including address information for said electronic content and time information for said proof in the certificate** (DeBry: Fig. 2 and col 7 lines 20-31 "The will-call certificate 40 (FIG. 2) contains the following fields: distinguished name of the document source 41, which tells the print

server exactly where to go to get the document (e.g., including the Internet address); the path to the document file 42 to find the document within the file system; and the digital signature of the provider of the document 43. When the document source created the will-call certificate, the document source digitally signed the will-call certificate using its own private key. The will-call certificate also contains a date indicating a date until which the certificate is valid 44, and a serial number for tracking purposes 45. ")

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of including address information for said electronic content and time information for said proof in the certificate in the system of Vaeth and Kobata, as DeBry teaches so as to securely retrieve a file.

The combination of Vaeth, Kobata and DeBry does not disclose "**synchronizing clocks of said proof service provider with said witness";** however, Van der Kaay discloses this limitation. (see Van der Kaay col 2 lines 40-42 " a Time Calibration Certificate (TCCert), as used herein, which relates to the certification of a clock as synchronized with an accepted standard." And col 8 line 65 to col 9 line 24 "The NOC 210 comprises three additional functional components that implement the PKI authentication capability of the TTI system. The Registration Authority (RA) 312 associates each device in the TTI system with a name. In this manner, TTI devices can be identified, monitored, and controlled. The Certification Authority (CA) 314 associates a public key with each device using the name of the device provided by the RA 312....the NOC 210 acts as an RA 312 to the CA 314 for the issuance of digital certificates to the TTI elements. Each

element within the TTI preferably has a distinguished name so that it may be uniquely identified.")

Van der Kaay discloses a Trusted Time Infrastructure (TTI) system provides time stamps, in the form of trusted temporal tokens, for electronic documents from a local source.A preferred embodiment of the system comprises a trusted master clock, a trusted local clock, and a network operations center. The trusted master clock and the network operations center are located within secure environments controlled by a trusted third party. The trusted local clock, which issues time stamps, is certified to be synchronized with the trusted master clock. (see Van der Kaay col 4 lines 40-51)

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the synchronizing clocks of said proof service provider with said witness (e.g. CA and RA) as taught by Van der Kaay to modify the modified-invention of Vaeth because there are in the same field of endeavor of authentication for certification so as to securely verifying, processing, and storing the electronic content.

As for claim 11:

The combination of Vaeth, Kobata, DeBry and Van der Kaay discloses **the proving system according to claim 10, wherein said certificate includes said electronic content, or data that uniquely represent said electronic content.** (see Vaeth: Fig.1, col. 3, lines 35-41 "the CA provides a certificate including (a) information identifying the certified party, (b) the certified party's public key, and (c) information identifying the CA, digitally signed, that is, encrypted with the CA's private key. The certified party can send such a certificate.").

As for claim 12:

The combination of Vaeth, Kobata, DeBry and Van der Kaay discloses **the proving system according to claim 10, further comprising means for accumulating said certificate in a computer system of said service provider or means for transmitting said certificate to a user.** (see Vaeth col 8 lines 49-51 "storing the certificate at 191, and notifying requester 170 of the availability of the certificate, for example, by e-mail over network 200.")

As for claim 14:

The combination of Vaeth, Kobata, DeBry and Van der Kaay discloses **the proving system according to claim 10, wherein said means for generating said certificate includes means for providing a signature for said certificate; wherein said means for providing a signature includes a first configuration~ consisting of first signature means by said witness or said certificate generator and second signature means by said service provider, or a second configuration consisting of signature means by a notary service provider.** (see Vaeth col. 4, lines 41-47 "LRA 80 then accepts CRD 73, checks it for errors or omissions and verifies the requester's signature, submitting it to CA 90 in a message signed by LRA 80 using secure means 81. CA 90 validates the request for a certificate, then prepares the certificate information, signs it with the CA's private key and distributes the certificate to subscribers 95")

As for claim 15:

The combination of Vaeth, Kobata, DeBry and Van der Kaay discloses **the proving system according to claim 14, wherein eneryption means using a public key encryption method is employed for said signature means to prevent alteration by a person other than a signer.** (see Vaeth col. 2, line 16 to col 3 line 13" General asymmetric or "public key" encryption/decryption mechanisms are well known in the art, such as those invented by Rivest, Shamir and Adleman ("RSA"). The concept is based upon the existence of algorithms that allow encryption/decryption using related "keys" that are associated with each other, but one of which, the "private" key, is extremely difficult to derive from the other, "public" key."; and col 3 lines 35-40 "the CA provides a certificate including (a) information identifying the certified party, (b) the certified party's public key, and (c) information identifying the CA, digitally signed, that is, encrypted with the CA's private key. The certified party can send such a certificate.").

As for claim 18:

Vaeth discloses **a system for a witness or a certificate generator that proves openness for perusal or non-alteration of an electronic content using a computer system or a computer network,** (see Vaeth col. 1, lines 10-13 " the field of secure telecommunications, and, more specifically, the issuance and management of "certificates" in such telecommunications, particularly in electronic commerce.") **comprising: means for accepting a certificate generation request from a user;** (see Vaeth col. 6, lines 19-21 "the RA (a) accessing the certificate request information via the network")

means for accessing an address of an electronic content included in said certificate generation request, and obtaining said electronic content;

means for generating a certificate including said electronic content, or code that uniquely represents said electronic content; and

means for transmitting said certificate to said service provider, wherein said certificate includes address information for said electronic content and time information for a proof;

means for verifying a user's identity by referring to a usage history to determine said user as an authenticated user; (see Vaeth col. 4, lines 18-26 “Where the registration database has been created and historically maintained and used independently of the use of a CA, for example, a credit card issuer's databases of credit card holders and merchants, the maintainer of the database likely has more experience with for verification of the identity of the party.” And col. 2, lines 40-45 “By applying this type of encryption to a shortened, unique representation of a communication generated by a "hash function", a "digital signature" can be generated that authenticates to holders of the public key that the sender/encoder of the communication is the holder of the associated private key.”)

means for verifying that a certificate has been prepared by said witness; (see Vaeth col. 4, lines 16-17 “the CA performs the identity verification function, albeit using the registration database.”) **means for requesting preparation of a certificate by said witness:** (see Vaeth col. 4, lines 4- 5“CAs could have a "registration authority" (RA) function, for example, registering who within an organization was authorized with

signing privileges relative to a certain level of transaction activity." And col 4 line 34-36 "Requester 70 employs a public/private key pair generator 71 to generate the key pair, then prepares a certificate request data (CRD) submission 73, signed with the requester's private key, and sends it to the LRA 80 using secure means 75.") **means for determining whether said witness has accepted said witness process;** (see Vaeth col. 6, lines 18-20 "the RA (a) accessing the certificate request information via the network, (b) approving the request, and (c) sending the approval to the CA via the network;") **means for synchronizing clocks of said proof service provider with said witness; and accepting said certificate from said witness.** (see Vaeth col. 4, lines 40-42 " LRA 80 then accepts CRD 73, checks it for errors or omissions and verifies the requester's signature, submitting it to CA 90 in a message signed by LRA 80 using secure means 81.") Vaeth discloses administering certificates digitally signed by a trusted entity (certificate authority) to ensure that certificated transactions are authenticated as that of a particular entity. Requests for a certificate, along with verification information, are directed to the certificate authority, where they are held and accessed by an entity having verification responsibilities (registration authority). (see Vaeth abstract). Vaeth teaches the CA and RA are proof service provider and witness as the claim limitation recites.

Vaeth does not disclose the step of the witness or certificate generator obtaining electronic content upon the receipt of the certificate generation request from the service provider. However, Kobata discloses **for transmitting digital information over a network** (Kobata: col. 1, lines 1-2 "transmitting digital information over a network")

comprising receiving system obtains digital information from a server system

(Kobata: Fig. 1; col. 3, lines 21-43; col. 4, lines 6-49).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of obtaining contents electronically as Kobata teaches in the system of Vaeth so as to save transmission bandwidth.

The combination of Vaeth and Kobata is silent on the teaching of including address information for said electronic content and time information for said proof in the certificate. DeBry is relied on for the teaching of **including address information for said electronic content and time information for said proof in the certificate**

(DeBry: Fig. 2 and col 7 lines 20-31 "The will-call certificate 40 (FIG. 2) contains the following fields: distinguished name of the document source 41, which tells the print server exactly where to go to get the document (e.g., including the Internet address); the path to the document file 42 to find the document within the file system; and the digital signature of the provider of the document 43. When the document source created the will-call certificate, the document source digitally signed the will-call certificate using its own private key. The will-call certificate also contains a date indicating a date until which the certificate is valid 44, and a serial number for tracking purposes 45. ")

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of including address information for said electronic content and time information for said proof in the certificate in the system of Vaeth and Kobata, as DeBry teaches so as to securely retrieve a file.

The combination of Vaeth, Kobata and DeBry does not disclose "**synchronizing clocks of said proof service provider with said witness";** however, Van der Kaay discloses this limitation. (see Van der Kaay col 2 lines 40-42 " a Time Calibration Certificate (TCCert), as used herein, which relates to the certification of a clock as synchronized with an accepted standard." And col 8 line 65 to col 9 line 24 "The NOC 210 comprises three additional functional components that implement the PKI authentication capability of the TTI system. The Registration Authority (RA) 312 associates each device in the TTI system with a name. In this manner, TTI devices can be identified, monitored, and controlled. The Certification Authority (CA) 314 associates a public key with each device using the name of the device provided by the RA 312....the NOC 210 acts as an RA 312 to the CA 314 for the issuance of digital certificates to the TTI elements. Each element within the TTI preferably has a distinguished name so that it may be uniquely identified.")

Van der Kaay discloses a Trusted Time Infrastructure (TTI) system provides time stamps, in the form of trusted temporal tokens, for electronic documents from a local source.A preferred embodiment of the system comprises a trusted master clock, a trusted local clock, and a network operations center. The trusted master clock and the network operations center are located within secure environments controlled by a trusted third party. The trusted local clock, which issues time stamps, is certified to be synchronized with the trusted master clock. (see Van der Kaay col 4 lines 40-51)

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the synchronizing clocks of said proof service provider with said

witness (e.g. CA and RA) as taught by Van der Kaay to modify the modified-invention of Vaeth because there are in the same field of endeavor of authentication for certification so as to securely verifying, processing, and storing the electronic content.

As for claim 19:

The combination of Vaeth, Kobata, DeBry and Van der Kaay discloses **the system according to claim 18, wherein said means 9 for generating said certificate includes means for providing an electronic signature for said certificate.** (see Vaeth col. 4, lines 41-47 "LRA 80 then accepts CRD 73, checks it for errors or omissions and verifies the requester's signature, submitting it to CA 90 in a message signed by LRA 80
using secure means 81. CA 90 validates the request for a certificate, then prepares the certificate information, signs it with the CA's private key and distributes the certificate to subscribers 95")

As for claim 20:

Vaeth discloses **a computer readable storage medium for storing a program code that proves openness for perusal and non-alteration of an electronic content using a computer system or a computer network,** (see Vaeth col. 1, lines 10-13 " the field of secure telecommunications, and, more specifically, the issuance and management of "certificates" in such telecommunications, particularly in electronic commerce.")**said program code comprising:**

a program code for, in accordance with a service request from a user or a self service request, transmitting a certificate generation request to a witness or a

certificate generator; (see Vaeth col. 6, lines 19-21 "the RA (a) accessing the certificate request information via the network") **a program code for obtaining electronic content upon the receipt of said certificate generation request from said service provider; a program code for generating a certificate that includes said electronic content, or data that uniquely represent said electronic content; and either a program code for accumulating said certificate in a computer system of said service provider or a program code for transmitting said certificate to a user, wherein said certificate includes address information for said electronic content and time information for a proof;**

a program code for verifying a user's identity by referring to a usage history to determine said user as an authenticated user; (see Vaeth col. 4, lines 18-26 "Where the registration database has been created and historically maintained and used independently of the use of a CA, for example, a credit card issuer's databases of credit card holders and merchants, the maintainer of the database likely has more experience with for verification of the identity of the party." And col. 2, lines 40-45 "By applying this type of encryption to a shortened, unique representation of a communication generated by a "hash function", a "digital signature" can be generated that authenticates to holders of the public key that the sender/encoder of the communication is the holder of the associated private key.")

a program code for verifying that a certificate has been prepared by said witness; (see Vaeth col. 4, lines 16-17 "the CA performs the identity verification function, albeit using the registration database.")

a program code for requesting preparation of a certificate by said witness; (see Vaeth col. 4, lines 4- 5"CAs could have a "registration authority" (RA) function, for example, registering who within an organization was authorized with signing privileges relative to a certain level of transaction activity." And col 4 line 34-36 "Requester 70 employs a public/private key pair generator 71 to generate the key pair, then prepares a certificate request data (CRD) submission 73, signed with the requester's private key, and sends it to the LRA 80 using secure means 75.")

a program code for determining whether said witness has accepted said witness process; (see Vaeth col. 6, lines 18-20 "the RA (a) accessing the certificate request information via the network, (b) approving the request, and (c) sending the approval to the CA via the network;") **a program code for synchronizing clocks of said proof service provider with said witness; and a program code for accepting said certificate from said witness.** (see Vaeth col. 4, lines 40-42 " LRA 80 then accepts CRD 73, checks it for errors or omissions and verifies the requester's signature, submitting it to CA 90 in a message signed by LRA 80 using secure means 81.") Vaeth discloses administering certificates digitally signed by a trusted entity (certificate authority) to ensure that certificated transactions are authenticated as that of a particular entity. Requests for a certificate, along with verification information, are directed to the certificate authority, where they are held and accessed by an entity having verification responsibilities (registration authority). (see Vaeth abstract). Vaeth teaches the CA and RA are proof service provider and witness as the claim limitation recites.

Vaeth does not disclose the step of the witness or certificate generator obtaining electronic content upon the receipt of the certificate generation request from the service provider. However, Kobata discloses **for transmitting digital information over a network** (Kobata: col. 1, lines 1-2 “transmitting digital information over a network”) **comprising receiving system obtains digital information from a server system** (Kobata: Fig. 1; col. 3, lines 21-43; col. 4, lines 6-49).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of obtaining contents electronically as Kobata teaches in the system of Vaeth so as to save transmission bandwidth.

The combination of Vaeth and Kobata is silent on the teaching of including address information for said electronic content and time information for said proof in the certificate. DeBry is relied on for the teaching of **including address information for said electronic content and time information for said proof in the certificate** (DeBry: Fig. 2 and col 7 lines 20-31 “The will-call certificate 40 (FIG. 2) contains the following fields: distinguished name of the document source 41, which tells the print server exactly where to go to get the document (e.g., including the Internet address); the path to the document file 42 to find the document within the file system; and the digital signature of the provider of the document 43. When the document source created the will-call certificate, the document source digitally signed the will-call certificate using its own private key. The will-call certificate also contains a date indicating a date until which the certificate is valid 44, and a serial number for tracking purposes 45. “)

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of including address information for said electronic content and time information for said proof in the certificate in the system of Vaeth and Kobata, as DeBry teaches so as to securely retrieve a file.

The combination of Vaeth, Kobata and DeBry does not disclose "**synchronizing clocks of said proof service provider with said witness";** however, Van der Kaay discloses this limitation. (see Van der Kaay col 2 lines 40-42 " a Time Calibration Certificate (TCCert), as used herein, which relates to the certification of a clock as synchronized with an accepted standard." And col 8 line 65 to col 9 line 24 "The NOC 210 comprises three additional functional components that implement the PKI authentication capability of the TTI system. The Registration Authority (RA) 312 associates each device in the TTI system with a name. In this manner, TTI devices can be identified, monitored, and controlled. The Certification Authority (CA) 314 associates a public key with each device using the name of the device provided by the RA 312....the NOC 210 acts as an RA 312 to the CA 314 for the issuance of digital certificates to the TTI elements. Each element within the TTI preferably has a distinguished name so that it may be uniquely identified.")

Van der Kaay discloses a Trusted Time Infrastructure (TTI) system provides time stamps, in the form of trusted temporal tokens, for electronic documents from a local source.A preferred embodiment of the system comprises a trusted master clock, a

trusted local clock, and a network operations center. The trusted master clock and the network operations center are located within secure environments controlled by a trusted third party.The trusted local clock, which issues time stamps, is certified to be synchronized with the trusted master clock. (see Van der Kaay col 4 lines 40-51) Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the synchronizing clocks of said proof service provider with said witness (e.g. CA and RA) as taught by Van der Kaay to modify the modified-invention of Vaeth because there are in the same field of endeavor of authentication for certification so as to securely verifying, processing, and storing the electronic content.

As for claim 21:

The combination of Vaeth, Kobata, DeBry and Van der Kaay discloses **an article of manufacture comprising a computer readable storage medium having computer readable program code means embodied therein for causing an electronic content proving method, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 1.** (Please see above on the claim 1)

As for claim 22:

The combination of Vaeth, Kobata, DeBry and Van der Kaay discloses **a computer program product comprising a computer readable storage, medium having computer readable program code means embodied therein for causing a proving system, the computer readable program code means in said computer program**

product comprising computer readable program code means for causing a computer to effect the system of claim 10. (Please see above on the claim 10)

As for claim 24:

The combination of Vaeth, Kobata, DeBry and Van der Kaay discloses **a computer program product comprising a computer readable storage medium having computer readable program code means embodied therein for causing proof of openness for perusal or non-alteration of an electronic content, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the system of claim 18.** (Please see above on the claim 18)

7. Claims 16 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vaeth et al (6,308,277); in view of Lim (6,728,884), in view of DeBry (6,385,728) and further in view of Van der Kaay et al (US 6,393,126 B1).

As for claim 16:

Vaeth discloses **a proving system for a service provider that proves openness for perusal or non-alteration of an electronic content using a computer system or a computer network,** (see Vaeth col. 1, lines 10-13 " the field of secure telecommunications, and, more specifically, the issuance and management of "certificates" in such telecommunications, particularly in electronic commerce.") **comprising: means for accepting and for analyzing a service request received from a user;** (see Vaeth Fig. 2, element 75); **means for selecting a witness or a**

certificate generator from a registered member group in which witnesses or certificate generators are registered;

means for transmitting a certificate generation request to said witness or said certificate generator that is selected; (see Vaeth Fig. 2, element 81);

means for accepting a certificate from said witness or from said certificate generator; (see Vaeth Fig. 2, element 83);**and**

means for transmitting said certificate to said user, (see Vaeth Fig. 2, element 77);

wherein said certificate includes address information for said electronic content and time information for a proof;

means for verifying a user's identity by referring to a usage history to determine said user as an authenticated user; (see Vaeth col. 4, lines 18-26 "Where the registration database has been created and historically maintained and used independently of the use of a CA, for example, a credit card issuer's databases of credit card holders and merchants, the maintainer of the database likely has more experience with for verification of the identity of the party." And col. 2, lines 40-45 "By applying this type of encryption to a shortened, unique representation of a communication generated by a "hash function", a "digital signature" can be generated that authenticates to holders of the public key that the sender/encoder of the communication is the holder of the associated private key.")

means for verifying that a certificate has been prepared by said witness; (see Vaeth col. 4, lines 16-17 "the CA performs the identity verification function, albeit using the registration database.") **means for requesting preparation of a certificate by said**

witness; (see Vaeth col. 4, lines 4- 5"CAs could have a "registration authority" (RA) function, for example, registering who within an organization was authorized with signing privileges relative to a certain level of transaction activity." And col 4 line 34-36 "Requester 70 employs a public/private key pair generator 71 to generate the key pair, then prepares a certificate request data (CRD) submission 73, signed with the requester's private key, and sends it to the LRA 80 using secure means 75.") **means for determining whether said witness has accepted said witness process;** (see Vaeth col. 6, lines 18-20 "the RA (a) accessing the certificate request information via the network, (b) approving the request, and (c) sending the approval to the CA via the network;") **means for synchronizing clocks of said proof service provider with said witness; and accepting said certificate from said witness.** (see Vaeth col. 4, lines 40-42 " LRA 80 then accepts CRD 73, checks it for errors or omissions and verifies the requester's signature, submitting it to CA 90 in a message signed by LRA 80 using secure means 81.") Vaeth discloses administering certificates digitally signed by a trusted entity (certificate authority) to ensure that certificated transactions are authenticated as that of a particular entity. Requests for a certificate, along with verification information, are directed to the certificate authority, where they are held and accessed by an entity having verification responsibilities (registration authority). (see Vaeth abstract). Vaeth teaches the CA and RA are proof service provider and witness as the claim limitation recites.

Vaeth does not disclose means for selecting a witness or a certificate generator from a registered member group.

Lim discloses a method and apparatus for selectively authenticating and authorizing a client seeking access to one or more protected computer systems over a network comprising means for selecting a name that corresponds to a proxy server from the plurality of proxy servers to authenticate user (col. 9, lines 58-67 to col. 10, lines 1-5).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of selecting a certificate generator or witness i.e proxy server from a plurality of proxy servers as Lim teaches in the system of Vaeth so as to guarantee the randomness and fairness in authenticating and authorizing users.

The combination of Vaeth and Lim is silent on the teaching of including address information for said electronic content and time information for said proof in the certificate.

DeBry is relied on for the teaching of including address information for said electronic content and time information for said proof in the certificate (DeBry: Fig. 2, elements 42 and 44).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of including address information for said electronic content and time information for said proof in the certificate in the system of Vaeth and Lim, as DeBry teaches so as to securely retrieve a file.

The combination of Vaeth, Lim and DeBry does not disclose "**synchronizing clocks of said proof service provider with said witness";** however, Van der Kaay discloses this limitation. (see Van der Kaay col 2 lines 40-42 " a Time Calibration Certificate (TCCert), as used herein, which relates to the certification of a clock as synchronized

with an accepted standard." And col 8 line 65 to col 9 line 24 "The NOC 210 comprises three additional functional components that implement the PKI authentication capability of the TTI system. The Registration Authority (RA) 312 associates each device in the TTI system with a name. In this manner, TTI devices can be identified, monitored, and controlled. The Certification Authority (CA) 314 associates a public key with each device using the name of the device provided by the RA 312....the NOC 210 acts as an RA 312 to the CA 314 for the issuance of digital certificates to the TTI elements. Each element within the TTI preferably has a distinguished name so that it may be uniquely identified.")

Van der Kaay discloses a Trusted Time Infrastructure (TTI) system provides time stamps, in the form of trusted temporal tokens, for electronic documents from a local source.A preferred embodiment of the system comprises a trusted master clock, a trusted local clock, and a network operations center. The trusted master clock and the network operations center are located within secure environments controlled by a trusted third party.The trusted local clock, which issues time stamps, is certified to be synchronized with the trusted master clock. (see Van der Kaay col 4 lines 40-51)

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the synchronizing clocks of said proof service provider with said witness (e.g. CA and RA) as taught by Van der Kaay to modify the modified-invention of Vaeth because there are in the same field of endeavor of authentication for certification so as to securely verifying, processing, and storing the electronic content.

As for claim 23:

The combination of Vaeth, Lim, DeBry and Van der Kaay discloses **a computer program product comprising a computer readable storage medium having computer readable program code means embodied therein for causing a proving system, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the system of claim 16.** (Please see above on the claim 16)

8. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vaeth, Lim, DeBry and Van der Kaay as applied to claim 16 above, further in view of Kohl et al. (6,430,688).

As for claim 17:

The combination of Vaeth, Lim, DeBry and Van der Kaay discloses **the proving system according to-claim 16** as above, none of them discloses **wherein said means for accepting said certificate includes means for providing an electronic signature for said certificate.** However, Kohl discloses issuing digital certificates to a client comprising digital signatures incorporate into a certificate (see Kohl col. 5, lines 37-43)

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of incorporating digital signatures into a certificate as Kohl teaches in the modified-system of Vaeth so as to ensure the authenticity.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JASON LEE whose telephone number is (571)270-7477. The examiner can normally be reached on Monday-Friday 9/5/4 (altering Friday off).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi T Arani can be reached on (571)272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/J. L./
Examiner, Art Unit 2438

/Taghi T. Arani/

Supervisory Patent Examiner, Art Unit 2438